STIP 03
AUGUST 2015

Wilson Center

SCIENCE + TECHNOLOGY INNOVATION PROGRAM

by Daniel Sui
James Caverlee
Dakota Rudesill

THE DEEP WEB AND THE DARKNET:

A LOOK INSIDE THE INTERNET'S MASSIVE BLACK BOX

Wilson Center

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue, NW
Washington, DC 20004-3027
(202) 691-4000, fax (202) 691-4001
www.wilsoncenter.org

About the Authors

Daniel Sui is Distinguished Professor of Social & Behavioral Sciences and was the Chair of the Geography Department (2011-2015) at The Ohio State University. His research focuses on the legal and ethical issues of technological innovations and his on-going projects examine the detection of location spoofing in location-based social media. He is currently a co-leader of the Climate, Security, Health and Resilience Initiative at Ohio State. Sui was a 2009 Guggenheim Fellow and 2015 Public Policy Scholar at the Woodrow Wilson International Center for Scholars.

James Caverlee is Associate Professor in the Department of Computer Science and Engineering at Texas A&M University. His research focuses on web-scale information management, distributed data- intensive systems, and social computing. He is a leader in understanding the spam and "crowdturfing" threats to social media and web systems, as well geo-social systems that leverage large-scale spatio-temporal footprints in social media.

Dakota Rudesill is Assistant Professor of Law at the Moritz College of Law at The Ohio State University. Over his two decade career, he has advised senior leaders throughout the federal government, including the Director of National Intelligence, the Chairman of the Senate Budget Committee, and Chief Judge of the Eighth Circuit Court of Appeals. He has been a visiting professor at Georgetown University Law Center, a visiting fellow at the Center for Strategic & International Studies, and was selected for the Council on Foreign Relations International Affairs Fellowship.

Our Mission

The mission of the Science and Technology Innovation Program (STIP) is to explore the scientific and technological frontier, stimulating discovery and bringing new tools to bear on public policy challenges that emerge as science advances. We work across a range of issues from strategic planning to risk management, technology assessment to regulatory reinvention, both domestically and internationally.

Project areas include: nanotechnology, synthetic biology, citizen science and crowdsourcing, serious games, participatory technology assessment, transformative social networking, and geo-engineering.

Disclaimer: The views and opinions expressed in this brief are those of the authors and do not necessarily reflect the official policy or position of STIP or the Wilson Center. Guidelines for accessing the Deep Web and Darknet are being provided in this brief for research and educational purposes only. Neither the authors nor the Wilson Center assume any responsibility for consequences resulting from use of information obtained at linked sites and are not responsible for, and expressly disclaim all liability for, damages of any kind arising out of use, reference to, or reliance on such information.

Contact us:

Science and Technology Innovation Program
Woodrow Wilson Center
One Woodrow Wilson Plaza
1300 Pennsylvania Ave., N.W.
Washington, D.C. 20004-3027
Email: stip@wilsoncenter.org
Tel: 202-691-4398

Summary

Many believe a Google search can identify most of the information available on the Internet on a given subject. But there is an entire online world – a massive one – beyond the reach of Google or any other search engine. Policymakers should take a cue from prosecutors – who just convicted one of its masterminds – and start giving it some attention.

The scale of the Internet's underworld is immense. The number of non-indexed web sites, known as the **Deep Web**, is estimated to be 400 to 500 times larger than the surface web of indexed, searchable web sites. And the Deep Web is where the dark side of the Internet flourishes. While there are plenty of law-abiding citizens and well-intentioned individuals (such as journalists, political dissidents, and whistleblowers) who conduct their online activities below the surface, the part of the Deep Web known as the **Darknet** has become a conduit for illegal and often dangerous activities.

This policy brief outlines what the Deep Web and Darknet are, how they are accessed, and why we should care about them. For policymakers, the continuing growth of the Deep Web in general and the accelerated expansion of the Darknet in particular pose new policy challenges. The response to these challenges may have profound implications for civil liberties, national security, and the global economy at large.

The Deep Web and The Darknet

THE DARKNET SURFACES

Although the concepts of the Deep Web and the Darknet have been in existence since the World Wide Web became popular in the mid-1990s, the growth of the Deep Web and Darknet did not gain broader public attention until the arrest of the "Dread Pirate Roberts," also known as Ross William Ulbricht, in October 2013. Ulbricht gave "Silk Road" a new meaning to the public as the creator and operator of an online marketplace of the same name, where users could find all manner of contraband, particularly illegal drugs (Konrad, A. 2013). The FBI estimated that the Silk Road marketplace had processed more than $1.2 billion in sales by July 2013 involving 150,000 anonymous customers and around 4,000 vendors (Bartlett, J. 2015). The Deep Web and Darknet have also quickly become fixtures in popular culture, playing a key role in the U.S. *House of Cards* series, when a reporter uses it to hire a hacker to dig up dirt about the Vice President. More recently, the Deep Web is also the theme of a new documentary by Alex Winter about Ulbricht, who was eventually convicted of a series of federal crimes related to his black market activities (Weisner, B. 2015).

It is not the first time Hollywood has played an important role airing issues surrounding emerging technology. From Frit Lang's 1927 film *Metropolis* to Stanley Kubrik's 1968 movie *2001: A Space Odyssey* to Steven Spielberg's 2002 blockbuster *Minority Report*, film and television have explored the potential social impacts (intended or unintended) of technological advancements, from automobiles to space exploration to biotech and artificial intelligence. With the Deep Web, Hollywood is ahead of the scholarly and policy community in raising public awareness of the multi-faceted implications of the rapidly expanding unindexed Internet. But policymakers and scholars must catch up. In this policy brief, we provide an introduction on the Deep Web and Darknet, how they are accessed, and why policymakers should care about them.

THE DEEP WEB AND DARKNET, DEFINED

If we conceive of the Web as a data ocean, most of us are interacting with the wavy, transparent, easily navigable Surface Web (see Figure 1). The Surface Web is the portion of the Web that has been crawled and indexed (and thus searchable) by standard search engines such as Google or Bing via a regular web browser. In the darkness below, beneath the electronic thermocline, are the abyssal depths of the Deep Web (also referred to as the Invisible Web or Hidden Web) – the portion of the web that has not been crawled and indexed, and thus is beyond the sonar reach of standard search engines. It is technically impossible to estimate accurately the size of the Deep Web. However, it is telling that Google – currently the largest search engine – has only indexed 4-16 percent of the Surface Web. The Deep Web is approximately 400-500 times more massive than the Surface Web (See brightplanet.com). It is estimated that the data stored on just the 60 largest Deep Web sites alone are 40 times larger than the size of the entire Surface Web (See thehiddenwiki.net).

FIGURE 1. The Surface Web vs. the Deep Web

[Source: Brand Powder, http://www.brandpowder.com/how-deep-is-your-web/
Used with permission]

Growing rapidly within the Deep Web is the Darknet (also referred to as the Dark Web, Dark Net, or Dark Internet). Originally, the Darknet referred to any or all network hosts that could not be reached by the Internet. However, once users of these network hosts started sharing files (often anonymously) over a distributed network that was not indexed by standard search engines, the Darknet became a key part of the Deep Web. Unlike the traffic on the Surface Web or most parts of the Deep Web, most Darknet sites can only be accessed anonymously.

Preliminary studies have revealed that the Deep Web actually contains the largest expanding reservoir of fresh information on the Internet.

These websites are usually narrower, but with much deeper content material, as compared to regular surface sites. Furthermore, because most of the materials are protected content, the overall quality of the content from the Deep Web is typically better and more valuable than that of the Surface Web. It is also estimated that more than 50 percent of the Deep Web content is located in topic-specific directories (www.thehiddenwiki.net), making it even more accessible and relevant to targeted searches.

And the Deep Web and Darknet are growing. Multiple technologies, such as ubiquitous computing, distributed/cloud computing, mobile computing, and sensor networks, have all contributed to the expansion of the Deep Web. Advances in secure/anonymous web hosting services, cryptocurrency/Dark Wallet, and development of crimeware are further contributing to the growth of the Darknet. A variety of cryptocurrencies such as Bitcoin, Darkcoin, or Peercoin (see coinmarketcap.com for a complete listing) have been in use for anonymous business transactions that are conducted within and across most Darknet marketplaces. Hackers for hire and multilingual call centers have also accelerated the growth of Darknet. Of course, there are also plenty of legitimate uses of the Darket by journalists, political dissidents, whistle-blowers, and human rights advocates. Not surprisingly, Chelsea (formerly Bradley) Manning, Julian Assange, and Edward Snowden all relied heavily on the Darknet for their cause and activities.

HOW TO ACCESS THE DEEP WEB AND DARKNET

When film director James Cameron succeeded in a record-breaking dive to the deepest point of world's ocean, he tweeted: "Hitting bottom never felt so good. Can't wait to share what I'm seeing w/ you." But to get to the bottom of the Mariana Trench, Cameron relied on a custom-built submersible vehicle. By the same token, to explore the Deep Web and Darknet, we need some special tools and techniques. Some of them are similar to or closely related to those we use to explore the Surface Web.

Depending on one's overall goals, different tools and techniques will help reach different depths. For most users, there are generally two different but related approaches to access the Deep Web and Darknet:

- Use special search engines accessed from regular browsers such as Internet Explorer, Firefox, Chrome, Safari, etc.
- Use special search engines that can be accessed only from a TOR browser.

The research community and those familiar with technology can go even deeper by developing a custom-built crawling program using link-crawling techniques and API programming skills.

One easy way to gain access to the Deep Web is to use alternative/special search engines that are designed specifically for the purpose. These alternative search engines are designed to access different parts of the Deep Web (see Table 1), but the challenge is that all search engines developed so far only crawl or index a small part of the Deep Web. Therefore, it is still necessary to visit the right online directory or hidden web site listings (e.g. https://sites.google.com/site/howtoaccessthedeepnet/working-links-to-the-deep-web). Since these websites are not indexed, they will not be found using normal search tools. However, their URLs can be found using other means and, once the

URL is known, one can then access some of these sites on the Deep Web using regular browsers.

Some public databases are considered part of the Deep Web because most of their content cannot be crawled or indexed by usual search engines. For most users, they may be interacting with part of the Deep Web regularly, but they may not be aware of it. For example, the directory of the U.S. Library of Congress (www.loc.gov) is an online database that resides on the Deep Web. Other sites utilizing the Deep Web include economic data site FreeLunch.com, Census.gov, Copyright.gov, PubMed, Web of Science, WWW Virtual Library, Directory of Open Access Journals, FindLaw, and Wolfram Alpha.

In addition to these publicly available databases, there are plenty of pay-to-use databases (such as Westlaw and LexisNexis) and subscription-only services (found at most academic libraries) that utilize the Deep Web. One can only have access to these databases if they subscribe to them. In addition, there is also a vast amount of information that is private and password-protected (such as credit card and PayPal accounts) located on the Deep Web. Access to this part of the Deep Web is technologically restricted and legally protected.

With the prevalence of Web 2.0 and smartphone devices, a plethora of information is stored in various social networks that are generally not accessible through regular search engines. Many of them require users to be authorized (via registration or by becoming friends with other people) to access the data. Some of these services, like Twitter and Facebook, provide a public application program interface, or API, so that users can acquire the information in the network at a vast scale. But many of them, like YikYak and Wechat (both require log-in ID), limit users' accessibility to their massive database for reasons of security and privacy.

Instant messaging (IM) is another cistern of information in the Deep Web. Previously taking the form of online chatrooms, IM services provide a private and convenient space for people to exchange information, which is usually person-to-person and not archived. This is widely used in online chatting and technical support. Nowadays, some mobile applications allow users to save their messaging history locally so that they can be accessed later if necessary. In addition, instant messaging is becoming more multimedia based, making it harder to archive the messaging history. To access this part of the Deep Web, the best way to record the information is while the conversation is taking place, via screenshots or videotaping.

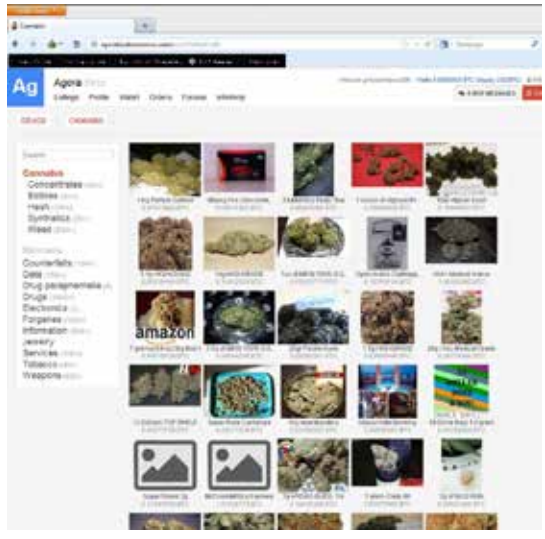
The Darknet has been increasingly used for trades, conversations, and information/file sharing and transfer in recent years because users are capable of maintaining anonymity, keeping their online activities private. To access the anonymous sites of the Deep Web, visitors must use a TOR (The Onion Router) browser (https://www.torproject.org/projects/torbrowser.html.en) to access websites with the ".onion" domain. Different from Surface Web browsers, the TOR browser allows users to connect to web pages anonymously, making it extremely difficult for anyone to track one's online activities if one follows all the protocols as required by TOR. Unlike the Surface Web, Darknet pages on the TOR network tend to be unreliable, often going down for hours or days or sometimes

disappearing permanently. They can also be very slow to load, since TOR is routing the connection through randomly selected servers to protect anonymity. While TOR browsers exist for Android and iOS, these are not secure and not recommended. Similarly, TOR add-ons for other browsers are not secure and are usually not supported by the TOR organization, thus not recommended either.

Since the arrest of Ulbricht in 2013, dozens of Silk Road replacements have sprung up Medusa-like as hidden services deployed on the TOR network. A new and improved version of Silk Road, called Silk Road 2.0, sprung up and was shut down again by law enforcement agencies in November 2013. Figure 4 shows a sample listing under the "Drugs" category on the Agora Darknet marketplace. Among the thousands of listings under this category are advertisements for MDMA, cocaine, Oxycodone, and heroin, among others. Just as on eBay and Amazon, sellers receive feedback scores from their customers, including detailed comments about the quality of the product, delivery time, and other related e-commerce metrics. Indeed, just as the growth of the web "flattened" informational flows, these Darknet marketplaces represent a fundamental shift in the illicit underground economy towards enabling worldwide access and distribution of products and services that have historically required significant investments in the "last mile" of the supply chain. This disruption creates the potential for massive shifts in the international supply chain of goods and services, particularly those that are illegal or subject to taxation or other forms of regulation.

While the Darknet gained notoriety for illegal activities, there are myriad legitimate and benign uses for law-abiding citizens as well. Some are based on familiar concepts, like image

FIGURE 2. Example of Drug Listings from the Agora Marketplace



[Source: Agora Marketplace, screen capture by Dakota Rudesill]

sharing (e.g., http://www.zw3crggtadila2sg.onion/imageboard/), which take advantage of the increased security provided by the Deep Web. Others are more unique to Deep Web culture, such as secure whistleblowing sites (e.g., http://5r4bjnjug3apqdii.onion/) and eBook collections focused on subversive works (e.g., https://xfmro77i3lixucja.onion.lt/). Journalists have used SecureDrop or GlobalLeaks to share files via the TOR network. Public accounts indicate that Chelsea Manning, Julian Assange, and Edward Snowden all used the TOR network one way or the other to share the massive troves of classified U.S. government files before they leaked them online.

To combat illegal activity on the Darknet, many law enforcement groups have adopted the practices and techniques of online criminals and many network investigative techniques, as they are called by law enforcement agencies, are often

similar or identical to routine hacking techniques (Ablon et al., 2014; Mckinnon, 2015). To pierce the dense layers of the anonymity offered by TOR, the Federal Bureau of Investigation (FBI) used a powerful app called Metasploit in "Operation Torpedo," a 2012 sting against the users of three Darknet child pornography websites. The FBI also participated in an international legal effort codenamed "Operation Onymous" last year using similar hacking techniques and malware. Using these hacking techniques to study the Deep Web and Darknet raises perplexing legal and ethical questions for researchers due to privacy concerns and the possible violation of well-established Institutional Review Board (IRB) research protocols. Researchers run the risk of doing the wrong thing as they pursue legitimate research projects.

LEGAL IMPLICATIONS

For policymakers, the emergence of the Deep Web in general and Darknet in particular offers a new economic, social, and political ecosystem that was designed to exist – and usually operates – beyond the reach of law, regulation, and government oversight. If policymakers want to understand the Deep Web and Darknet, they will need to give it intentional focus and move beyond usual Internet search methods.

Underneath the Internet's noisy Surface Web are a cast of anonymized Darknet operators whose activities are of enormous concern to government and to the public: drug dealers, hackers, hitmen, hoaxers, human traffickers, pimps, child pornographers, identity thieves, money launderers, leakers, political extremists, vigilantes, terrorists, and spies. But beyond those engaged in criminal or highly questionable activity are well-intentioned individuals (including gamers, journalists, activists, and others) who simply want additional privacy. In the classic formulation of privacy advanced by Supreme Court Justice Louis Brandeis more than a century ago, this latter category of Deep Web dwellers simply wants to be left alone. This understandable and legitimate privacy interest in the Deep Web's anonymity (or at least greater user control over anonymity) does not mean that states should turn a blind eye to the entire Deep Web.

The reality is that while the Surface Web manifests an often astonishing level of altruism for promoting the common good, and the Deep Web inevitably does to some (unknown) extent as well, the Deep Web and Darknet quite often reveal the darker, more antisocial side of human behavior. The markets for hacking programs, other cybercrime tools, and stolen data, in particular, have continued to grow with no signs of slowing down. There an urgent need for policymakers and the public to better understand the Deep Web and develop a more comprehensive law enforcement, regulatory, and national security response. This focus needs also to take into account the potential positive uses of the Deep Web. For instance, in 2010 TOR received an award for Projects of Social Benefit from the Free Software Foundation for services it provides to whistleblowers and human rights supporters.

Darknet markets, by hiding the identities of those involved in transactions and often conducting business via Bitcoin, inherently represent illegality and regulatory evasion. As demonstrated by the Silk Road drug market and its successors, a massive number of Darknet transactions involve contraband. Even where otherwise legitimate goods and services are involved, Darknet transactions often represent an assortment of

national crimes, from tax evasion to failure to observe duties and other limitations on imports and exports.

EXISTING LEGAL FRAMEWORKS

The Darknet market for hacking software and other cybercrime tools presents a particularly serious problem. When utilized, hacking tools violate computer crime laws. In the United States, these include the Computer Fraud and Abuse Act (CFAA), which bans trespassing on, unauthorized accessing of, and damaging computers in interstate or international commerce (see 18 U.S.C. 1030(a)(2-5)). CFAA also bars trafficking in unauthorized computer access and computer espionage (see 18 U.S.C. 1030(a)(6)).

The international regulatory environment regarding illicit cyber activity is at an early stage of development. No treaty deals comprehensively with the insecurity created in part by the availability of hacking tools via the Darknet. It is true that international law enforcement cooperation generally is longstanding and can be brought to bear on the Darknet and other illicit cyber activities to the extent they violate national laws and trade agreements. Law enforcement cooperation has been facilitated by the cybercrime-focused 2001 Budapest Convention, also known as the Council of Europe Convention on Cybercrime. This accord endeavors to harmonize criminal laws and improve investigation and cooperation among law enforcement agencies internationally on matters including computer network security, computer-related forgery and fraud, child pornography, and copyright infringements. Notably, the Convention in Article 6 states that state parties shall criminalize the sale, procurement, import, and distribution of code and other hacking tools.

Despite the Budapest Convention's promise, however, the American Bar Association's Standing Committee on Law and National Security has observed that "information sharing across national boundaries is slow and limited" compared to the speed at which the illicit cyber realm operates. "Substantive convergence of the law is even further in the future and may well prove impossible," the association says. Differing national approaches to crime, combined with territorial limits on criminal jurisdiction and investigative authorities, tie legal regimes to geography in the context of an Internet and Darknet markets that are seemingly everywhere and nowhere.

Better understanding Darknet markets would facilitate better tailored and therefore more effective national-level responses by the United States and other nations and over time better international cooperation, as well. The Deep Web's depths harbor not only illegal transactions in traditional goods and services and the latest hacking tools, but are also a battlefield where cyberwar and cyberespionage are and increasingly will be waged (Goodman, 2015). As questions of international law and national security policy as practiced globally, there are no well-settled answers within the international community to the key questions of when a cyberattack rises to the level of an armed attack, when a cyberattack can be attributed to a state actor (particularly where the attacker masks their identity, location, and origins of the code they use in the attack, and the state from which the code was launched denies involvement), and what force used in response would be appropriate legally and operationally.

The non-binding Tallinn Manual, commissioned by the North Atlantic Treaty Organization and released in 2013, begins to address the legal element, as do a number of U.S. government and other national-level legal policy documents. However, international consensus remains elusive. Key states including Russia and China – named by the U.S. intelligence community as the top cyber threats globally – actively resist development of international norms. In the United States, Congress in statute and the Executive Branch in presidential guidance and other policy documents have made it clear that a cyberattack – whether from a state or non-state actor using hacking tools – can rise to the level of being a use of force and is accordingly subject to the law of armed conflict, also known as international humanitarian law or the law of war. Although diplomatic, law enforcement, and economic (regulatory) options are available in the event of a cyberattack, decision-makers may also consider overt or clandestine U.S. action in cyberspace by military or intelligence agencies against the Darknet activities of a non-state or state actor where the information available suggests a threat to national security. But again, international consensus on law and policy regarding cyberwar and cyberespionage is so far elusive.

In short, there are multiple regulatory issues related to the emerging Darknet at both national and international levels that need to be resolved. How well these issues are resolved will not only affect the cybersecurity of the United States and other states, but that of companies, individuals, and other private sector actors. The Deep Web and the Darknet implicate the future prosperity, governance, and fairness of the global order.

POLICY IMPLICATIONS

Focused data gathering and research, together with policymaker and public education, are prerequisites for quality systematic review and improvement of the existing regulatory framework at both national and international levels. Policy makers need to better understand the conditions that give rise to the Darknet and that are relevant to law enforcement, regulatory design, and national security. As a recent book highlighted, "… the Darknet is nothing more than a mirror of society. Distorted, magnified, and mutated by the strange and unnatural conditions of life online" (Bartlett, J. 2015). In particular, we would like to stress that policymakers should pay attention to the following:

- Socio-cultural forces are involved in the "generation and sustainability" of criminal entities that use the Darknet. For example, some countries do not have functioning or sufficient markets in legal goods, a context in which the Darknet may actually facilitate increased social welfare and economic efficiency. States in such a situation may have little incentive to enforce cybercrime laws, while free-riding on the law enforcement, regulatory, and national security efforts against truly bad actors carried out by other states.
- The Deep Web and the Darknet are attractive to many because of the prosecution, regulation, and national security surveillance efforts of states in the physical world and Surface Web. Illicit activity is being driven below the electronic thermocline of common search engines and usual investigative techniques, and states must be willing to dive beneath it to gather information and take action.

- The transnationality of these networks frustrates eradication, regulatory, and prosecution efforts of any one state, creating cooperation, collective action, and law harmonization problems for state actors attempting to work together to counter illicit use of the Internet.
- Rather than eradication, policymakers must focus systematically on bad actors and bad patterns, while striving to anticipate and favorably shape evolution of the Darknet. At times this effort might, like anti-terrorist efforts globally since 9/11, risk resembling "whack-a-mole" (the takedown of Silk Road represents one pelt). It will only succeed over time if a broader strategy including prevention, detection, and response is developed and followed with broad international participation and support.

REFERENCES

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* Santa Monica, CA.: Rand Corporation.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). *Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States.* Addiction, 109(5), 774-783.

Bartlett, J. (2015). *The Dark Net: Inside the Digital Underworld*. William Heinemann Ltd.

Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous.* London: Verso Books.

Goodman, M. 2015. *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*. New York: Random House.

Konrad, A. 2013, "Feds Say They've Arrested 'Dread Pirate Roberts,' Shut Down His Black Market 'The Silk Road,'" *Forbes*, October 2,

Mckinnon, A. 2015. *Hacking: Ultimate Hacking for Beginners.* Seattle, WA.: Amazon Digital Services.

Schneier, B. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton and Company.

Weisner, B. 2015. "Man Behind Silk Road Website Is Convicted on All Counts," *New York Times*, Feb. 4.

CONCLUSION

The Deep Web and the Darknet are an emerging *terra incognita* – a term first appeared in Ptolemy's Geography around AD 150 to refer to regions that have not been mapped or documented. Despite the great strides we have made in mapping the physical world, we still have a vast swathes of land yet to be fully documented. Similarly for the vast new virtual world defined by cyberspace, we have learned so much during the past 20 years or so. And yet, as the island of our knowledge expands, the shore of our ignorance also stretches. At the end of the day, with powerful search engines such as Google and Bing, what we have access to is only a small fraction at the surface of the gigantic data ocean. Indeed there is a vast terra incognita that still awaits us to explore.

Will we ever be able to hit the bottom and fully understand the Deep Web and the Darknet? We doubt it at this point for both technical and legal reasons, but it certainly requires much broader public debate and discussion on the multiple dimensions and impacts of the Deep Web as it is getting deeper and certain parts of it are getting darker by the day. Indeed, how to balance the protection of civil liberty for law-abiding citizens with the concerns for national security remains a daunting challenge for policymakers in the age of big data and Deep Web. But the first step is undoubtedly better information and a better understanding of the deepest stretches of the Internet.

TABLE 1. ALTERNATIVE SEARCH ENGINES AND TOOLS TO ACCESS THE DEEP WEB USING REGULAR BROWSERS

GENERAL SEARCH ENGINES AND DATABASES	**DeepDyve:** One of the newest search engines specifically targeted at exploring the Deep Web, available after signing up for a free membership.
	The Scout Archives: This database is the culmination of nine years' worth of compiling the best of the Internet.
	Silobreaker: This tool shows how the news impacts the global culture with current news stories, corresponding maps, graphs of trends, networks of related people or topics, and fact sheets,.
	OAIster: Search for digital items with this tool that provides 12 million resources from more than 800 repositories.
	Dogpile: Dogpile searches rely on several top search engines for the results then removes duplicates and strives to present only relevant results.
	SurfWax: This search engine works very well for reaching deep into the web for information.
	Mamma: Click on the Power Search option to customize the search experience with this meta-search engine.
SEMANTIC SEARCH TOOLS AND DATABASES	**Zotero:** Firefox users will like this add-on that helps organize research material by collecting, managing, and citing any references from the Internet.
	Freebase: This community-powered database includes information on millions of topics.
	Gnod: When searching for books, music, movies and people on this search engine, it remembers specified interests and focuses the search results in that direction.
	DBpedia: This semantic program allows users to ask complex questions and get results from within Wikipedia.

CUSTOM SEARCH ENGINES	**CustomSearchEngine.com:** This listing includes many of the Google custom search engines created.
	Custom Search Engines: There are three custom search engines here, two of which may be relevant for anyone interested in Utah constitution or juvenile justice.
	Figure Skating Custom Search Engine: Use this search engine to learn about figure skating, with results becoming more refined with increased use.
	Go Pets America Custom Search Engine: This search engine provides information on pets and animals, their health and wellness, jobs in the field, and more.
ACADEMIC AND SCIENCE SEARCH ENGINES	**WorldWideScience.org:** Search for science information with this connection to international science databases and portals.
	Science.gov: This government search engine offers specific categories including agriculture and food, biology and nature, Earth and ocean sciences, health and medicine, and more.
	MagBot: This search engine provides journal and magazine articles on topics relevant to students and teachers.
	HighWire Press: From Stanford University, this tool can access thousands of peer-reviewed journals and full-text articles.
COLLABORATIVE INFORMATION AND CROWDSOURCING DATABASES	**Del.icio.us:** As readers find interesting articles or blog posts, they can use this tool to tag, save, and share the content.
	Technorati: Not only is this site a blog search engine, but members can vote and share, thus increasing the visibility for blogs.
	Reddit: WPopular crowdsourced news and network site Reddit asks users to vote on articles, customizing content based on preferences.
	StumbleUpon: Users can "Stumble" Internet content by giving it a thumbs up or down, thereby customizing future content.

Source: Compiled by the authors by synthesizing information from the following: 1) http://www.searchengineguide.com; 2) http://deep-web.org/how-to-research/deep-web-search-engines; 3) http://www.online-college-blog.com/features/100-useful-tips-and-tools-to-research-the-deep-web; 4) http://www.wikihow.com/Search-the-Deep-Web

ACCESSING THE DARKNET:

Accessing the Darknet requires special tools and up-to-date information. The links below were active as of June 2015. ***Disclaimer:*** *Access guidelines are being provided for research and educational purposes only. Neither the authors nor the Wilson Center assume any responsibility for consequences resulting from use of information obtained at linked sites and are not responsible for, and expressly disclaim all liability for, damages of any kind arising out of use, reference to, or reliance on such information.*

- Install the TOR browser, which can be found at: https://www.torproject.org/projects/torbrowser.html.en.
- Once the TOR browser is installed, one easy starting place to access some of the Darknet sites is the hidden wiki (http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page), which collects Deep Web links. If the above URL is not accessible in the TOR Browser, one can try http://hwiki2tzj277eepp.onion/index.php?title=Main_Page or http://kpvz7kpmcmne52qf.onion/wiki/index.php/Main_Page.
- This area of the Deep Web loses major websites constantly, partly due to crackdowns on illegal activity and partly because many of the websites are run by individuals or small teams without any funding. To find out the latest replacements, check with other Deep Web users on OnionChat (http://www.chatrapi7fkbzczr.onion/).
- To further explore the Darknet, special search engines have been developed specifically for the TOR network. Darknet sites are intentionally difficult to explore and maintain, so these search engines may not be as effective as those on the Surface Web. In order to find a variety of results, a common practice is to use several different search engines for each search, such as Torch (http://xmh57jrzrnw6insl.onion/) or TorSearch (http://kbhpodhnfxl3clb4.onion/). Other options include Deep Search, Deep Dive, Deep Peep, and Duck Go. Particular attention should be paid to Grams, which is a special search engine developed specifically for searching the cyber black market. For any of these steps, one can also ask Surface Web communities for up-to-date instructions and advice.

One Woodrow Wilson Plaza
1300 Pennsylvania Avenue, NW
Washington, DC 20004-3027
202 / 691 / 4000
www.wilsoncenter.org